EXHIBIT 3

Freedom to Tinker

… is your freedom to understand, discuss, repair, and modify the technological devices you own.

« Immunize Yourself Against Sony's Dangerous Uninstaller
Does Sony's Copy Protection Infringe Copyrights? »

Not Again! Uninstaller for *Other* Sony DRM Also Opens Huge Security Hole

Thursday November 17, 2005 by J. Alex Halderman

I have good news and bad news about Sony's other CD DRM technology, the SunnComm MediaMax system. (For those keeping score at home, Ed and I have written a lot recently about Sony's XCP copy protection technology, but this post is about a separate system that Sony ships on other CDs.)

I wrote last weekend about SunnComm's spyware-like behavior. Sony CDs protected with their technology automatically install several megabytes of files without any meaningful notice or consent, silently phone home every time you play a protected album, and fail to include any uninstall option.

Here's the good news: As several readers have pointed out, SunnComm will provide a tool to uninstall their software if users pester them enough. Typically this requires at least two rounds of emails with the company's support staff.

Now the bad news: It turns out that the web-based uninstaller SunnComm provides opens up a major security hole very similar to the one created by the web-based uninstaller for Sony's other DRM, XCP, that we announced a few days ago. I have verified that it is possible for a malicious web site to use the SunnComm hole to take control of PCs where the uninstaller has been used. In fact, the the SunnComm problem is easier to exploit than the XCP uninstaller flaw.

To be clear, the SunnComm security flaw does not apply to the software that ships on CDs, but only to the uninstaller that SunnComm distributes separately for removing the CD software. So if you haven't used the uninstaller, you're not vulnerable to this flaw and you don't need to do anything.

If you visit the SunnComm uninstaller web page, you are prompted to accept a small software component—an ActiveX control called AxWebRemoveCtrl created by SunnComm. This control has a design flaw that allows any web site to cause it to download and execute code from an arbitrary URL. If you've used the SunnComm uninstaller, the vulnerable AxWebRemoveCtrl component is still on your computer, and if you later visit an evil web site, the site can use the flawed control to silently download, install, and run any software code it likes on your computer. The evil site could use this ability to cause severe damage, such as adding your PC to a botnet or erasing your hard disk.

You can tell whether the vulnerable control is installed on your computer by using our AxWebRemoveCtrl detector.

We have created a tool that will disable the control and/or block it from being installed. To apply our tool, download this file to a temporary location, then double click on the file's icon in Windows. (Windows may ask you to confirm that you wish to add the information in the file to the system registry–choose "Yes.") After the tool has been applied, you may delete the file you downloaded. The tool will take effect as soon as you close and restart Internet Explorer. We recommend that anyone who has used the SunnComm uninstaller run our tool as soon as possible.

Unfortunately, if you use our tool to block the control, you won't be able to use SunnComm's current uninstaller to remove their software. It's up to them to replace the flawed uninstaller with a safe one as soon as possible, and to contact those who have already used the vulnerable uninstaller with instructions for closing the hole.

UPDATE (Nov. 18): We are currently helping SunnComm test a new version of the uninstaller.

This entry was posted on Thursday November 17, 2005 at 1:46 pm and is filed under Security, DRM, Privacy, CD Copy Protection. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

49 Responses to "Not Again! Uninstaller for *Other* Sony DRM Also Opens Huge Security Hole"

1. *The PC Doctor* Says:
   November 17th, 2005 at 2:19 pm

   SunnComm MediaMax uninstaller causes security vulnerability too!

   Another bad day for Sony - Freedom to Tinker is reporting that the uninstaller for Sony's other DRM software, SunnComm's MediaMax, also opens up a security vulnerability on PCs that have used it.
   Ed and Alex over on Freedom to Tinke…

2. *Ken* Says:
   November 17th, 2005 at 3:22 pm

   Remember the good old days when Sony first started this madness? A bunch of kids discovered their efforts could be thwarted with a black marker pen. That's when we should have begun the boycott. I can picture a guy who looks a lot like Dr. Bunsen Honeydew slaving away at Sony's labs preparing to hit their evil customers with Phase IV in this ongoing war against The Dark Side. Did they ever think that their sales might not be dropping so much because of pirates? It may just be because so much of their catalog is rubbish.

3. *anonymous coward from /.* Says:
   November 17th, 2005 at 3:42 pm

   Okay, Sony infects pcs with rootkits to protect their IP. What about games that have the latest Starforce protection? Rootkits? For sure, crashes, drives disabled, Alcolhol and virtual drives get knocked out by Starforce protection. is this jus the tip of the iceberg?

4. *Avery J. Parker - Web site hosting and computer service* Says:
   November 17th, 2005 at 4:07 pm

   […] You almost want to bury your head in the sand at this point if you're Sony…. Freedom-to-tinker has some details. The last couple weeks the XCP copy protection that Sony uses has been the center of a Firestorm for rootkit capabilities and massive security problems. Well, it seems the OTHER Digital Rights Management (DRM) software they use (SunnComm MediaMax) has some serious flaws too. […]

5. *Life On the Wicked Stage: Act 2* Says:
   November 17th, 2005 at 4:14 pm

   More Bad News On The Sony DRM Front

   Just when you thought it was … Nah. You knew there was golng to be more. All the digging, researching, blogging, and handwringing over Sony's DRM Rootkit DRM Scheme obviously led to more digging, researching…etc…etc… on other DRM mechanisms. J.

6. *SettleUpSony»Blog Archive » Alex @ Freedom to Tinker: Other Sony DRM Also Opens Huge Security Hole* Says:
   November 17th, 2005 at 5:45 pm

   […] J. Alex Halderman and Ed Felten have been doing some great research on the dubious DRM uninstallers offered by Sony and the DRM vendors. It turns out that the uninstaller from SunnComm is flawed (see list of

CD's below). […]

7. *Jake* Says:
November 17th, 2005 at 5:54 pm

   I wonder if any of this will effect any of the ongoing blueray-HD/DVD discussions. It may be a matter of trust.

8. *Timanator* Says:
November 17th, 2005 at 5:58 pm

   We all know this is the tip of the iceburg. Spyware and adware often reduces new machines worth 2 thousand dollars to machines that perform the $80 range.

   I think think all companies that install software without concent need to be out of business, and their assets used to pay for enforcement.

9. *QrazyQat* Says:
November 17th, 2005 at 6:10 pm

   Gee, I'm so old I can remember when having a Sony product was a good thing.

10. *Steve* Says:
November 17th, 2005 at 6:12 pm

    Thank you for reporting this ridiculous BS, it's sad that my 20 years of good faith in Sony is now ruined over this DRM against people who actually pay for music buying cds - ridiculous…

11. *Abram* Says:
November 17th, 2005 at 6:16 pm

    All people must be stupid except Sony Genius which regards customer merely as morons. How much time did those victims waste restoring for their PC transmitting informations to Japan Sony Empire? Heroshima nuking done by US government is nothing to do with sincere customers like us….. But Trust is invaluable, and breach of trust done by Sony will certainly be judged by customers, not anyone else !

12. *Abram* Says:
November 17th, 2005 at 6:20 pm

    conpensation ? Sony and BMG will certainly go bankrupt ! because Trust is the greatest trade, but Trust is betrayed deliberately

13. *Kin* Says:
November 17th, 2005 at 8:10 pm

    im from the Philippines, and as of yesterday i still see some of sony-bmg's XCP CDs on the racks of tower records. is the sony recall just for the US?

14. *Erik* Says:
November 17th, 2005 at 8:24 pm

    Another way to deal with this sort of vunerability is to quite using trash known as IE.
    Get Opera, ActiveX vunerability gone, no hassle with specialized removal/blocking tools, web is faster, no worries.

15. *John Altermoede* Says:
November 17th, 2005 at 8:45 pm

If you want a list of CDs infected by SunnComm malware, they have a complete list on their website:

Just click “The CD in Question” pulldown near the bottom of this page.

http://www.sunncomm.com/support/askthetech.asp

16. *Tim Howland* Says:
November 17th, 2005 at 9:25 pm

While the glaring security holes in activex components have been obvious for a long long time now, it seems that a whole new class of vulnerability has been identified here. Active X components that do their jobs, require system access to do those jobs, and are intended to be one-shot applications instead are forced by the active X architecture to linger on indefinitely. While this isn’t a new attack, it certainly seems like there are plenty of people getting bit by it.

It seems like anyone who publishes what they think is a one-shot activeX component like this should be reviewing it in detail. Some obvious classes that probably need investigation probably include:

- Online updaters, as distributed by gaming companies (blizzard, maxis)
- anti-virus scanners from security companies (the in-browser kind)
- tax / financial software updaters

Is there a google query that can identify the GUID’s used to identify these components, and a simple test to track down which ones are “safe for scripting?” - it may be a good technique for getting them out of circulation quickly.

17. *BrianShih.com » More Sony DRM vulnerabilities* Says:
November 18th, 2005 at 12:39 am

[…] Okay… one more. Freedom to Tinker’s J. Alex Halderman is reporting another vulnerability related to Sony’s DRM that can be exploited. This time, it’s not the XCP software that’s causing the problem - it’s the other one: SunnComm’s MediaMax. Specifically, while MediaMax doesn’t cause as many problems when it’s installed, it does do several things that make it look a lot like spyware. But the real problem is if you run the uninstaller provided by SunnComm, it opens up a vulnerability that allows external computers to take over your PC. […]

18. *Vaidyanathan* Says:
November 18th, 2005 at 2:28 am

I am unable to understand sony’s logic. It goes something like this:
1. Assume all customers are filthy pirates.
2. So punish those sincere enuf to buy their CDs instead of going to torrents.
3. After enduring infections and computer crashes expect the same customers (and others) to buy more of similar trojan infected spyware CDs.
4. If they dont buy blame P2P networks.
5. Put more malware into the CDs in the name of copyright protection (i.e. point 2).
And go round and round in the vicious cycle…

19. *Sys Builder* Says:
November 18th, 2005 at 3:19 am

Why bother with Sony? Garbage Hardware, software, and support—I have completely eliminated ALL OF THEIR PRODUCTS from my system design and deployment. PERIOD> Vote with your wallet—NO MORE PS2, Cameras, TVs, etc—and all of their crappy propietary sofware and hardware! Ever try to get NERO to work properly with their CD Burners? And their tech support tries to give you some SONY software to “do the trick”?

I have never found any of SONY's products to be worth a damn—dump their crap, and get on board with other quality products. The balls that SONY has to even SELL CD/DVD burners after the @#$% THEY JUST PULLED—unbelievable!

20. *TheObviousChild* Says:
    November 18th, 2005 at 6:55 am

    Sys Builder Says:

    >Ever try to get NERO to work properly with their CD Burners? And >their tech support tries to give you some SONY software to "do the >trick"?

    Yes, and have never had any problems. You did take the little bit of cardboard out of the drive, and plug it in before using it, right? ☺

    OTOH, rising to the bait of blog flaming 'tards aside, even if Sony's past glories have been notable, I suspect that behaving in such a dishonest and cavalier attitude will lose them mindshare.

    They might have waited to shaft the public until after the launch of the PS3, all eyes will now be on SCEE, and very little hidden evil will now escape the gimlet eye of massed angry geeks.

21. *Sony Rootkit - Amazon.com risarcisce* Says:
    November 18th, 2005 at 7:27 am

    […] Nel frattempo, come se non bastasse, saltano fuori problemi di sicurezza relativi alla disinstallazione anche per un altro sistema DRM Sony … […]

22. *TomCS* Says:
    November 18th, 2005 at 8:02 am

    Great work. Could you now possibly do the same for the Sunncomm Mac version? OK, it doesn't autoload, but that only makes it a social engineering exploit.

    What does it do,where does it sit,does it phone home,does it fully uninstall,etc?

23. *The Nickel Arcade » Sony's DRM infringed copyright of infamous hacker* Says:
    November 18th, 2005 at 10:26 am

    […] In related news, Sony's other DRM software that is used on other CDs (called SunnComm MediaMax) also behaves like spyware (phones home when you play the CD and can't be uninstalled) and if you do manage to convince SunnComm to give you an uninstaller, it also opens giant security holes on your system. […]

24. *Howard, Devon, UK.* Says:
    November 18th, 2005 at 10:28 am

    Sony deserve disaster - pity the wrong people will then lose jobs as ever. They used to make great audio gear (I used it as a broadcasting pro and as a home user), then about 10 years back the rot set in and you got poor assembly quality, no real service, just insulting messages about consulting authorised repair dealers etc. Sony must smart up or go under.

25. *HCS's and Gen's Place » Blog Archive » Other Sony DRM Uninstaller Leaves Security Holes* Says:
    November 18th, 2005 at 11:04 am

    […] Freedom to Tinker » Blog Archive » Not Again! Uninstaller for Other Sony DRM Also Opens Huge Security Hole […]

26. *TPN :: The Microsoft Show » Blog Archive » Sony's other DRM uninstaller has a security whole* Says:
November 18th, 2005 at 12:05 pm

[…] From Free to Tinker: Here's the good news: As several readers have pointed out, SunnComm will provide a tool to uninstall their software if users pester them enough. Typically this requires at least two rounds of emails with the company's support staff. […]

27. *Steve* Says:
November 18th, 2005 at 5:20 pm

Please delete my most recent post. http://www.bbspot.com/News/2005/11/sony_photo_sharing.html is a spoof. My sense of humor must be off as I failed to recognize it as a spoof.

28. *briareus* Says:
November 18th, 2005 at 5:36 pm

The irony is fantastic:

Aren't *we* supposed to be the ones who cannot be trusted?

Aren't *we* the underhanded thieves using technology to infiltrate their revenue model?

Wasn't it the obtaining of music without paying for it that started all this mess?

Apparently, I am such an untrustworthy scheming thieving hacker-type that I deserve to have my machine rooted from a CD that I actually paid for. So much for customer, I am also apparently the enemy. Amazing!

On a tangential note, the day before I heard about all this, I proved their view incorrect: I downloaded a song from a band that gets no radio play, and I liked it. So i downloaded more from the same album. I liked them all alot. Two days later, I went to the record store and I bought the album. The Internet generated a sale, from nothing, from no radio play at all.

Put that in your pipe and smoke it, Sony.

…and that goes for the rest of the record companies who think the same, who just made me think twice about ever paying for a song again, ever.

29. *Freedom to Think* Says:
November 18th, 2005 at 10:36 pm

After all this talk about Sony & their XCP/Sunncomm, why have you not talked about DRM that Macrovision has been doing?

30. *Freedom to Think* Says:
November 18th, 2005 at 10:43 pm

Let's be fair about this, if you are going to talk/bash XCP and/or Mediamax, why don't you discuss Macrovision & their DRM? Could it be that you as "Princeton University computer science" student be partial to Macrovision as at least 1 of the their board member(s) was a Princeton alumni? Come on, if you want to talk about this, let's do it straight across the board!!!

31. *cglrcng* Says:
November 19th, 2005 at 12:51 am

Anyone else wish to join me in a class action suit?

I'm dead serious. I installed the phony rootkit removal tool labeled "Offline Software Updater" from First4InternetLtd "Update031105″ on 11-4-05 but reached it by going to the Sony/BMG site which sent me to the First4Internet site and downloaded and ran the Offline Updater File. I saw it install - not un-install…That Black Box flash is un-mistakable. I immediately reported that to the

Sony screwed up w/ me here bigtime…I build Custom Computers, update, repair, etc. and used almost strictly all Sony Drive products (Floppy, CD, CD-RW, DVD, CD/RW/DVD, Media Card Readers, etc.). I won't again. That is a big loss as I have more than a few customers.

I did run the Symantec Removal Tool later as the Active X item is not installed as shown by the check listed here earlier. I will assume it is removed by that removal tool. Since I use many anti-spyware tools I can't really be sure which one closed the huge security hole(s) Sony and thier Cronies opened up on MY BOX!

I will be trading in ALL MY SONY/BMG or BMG CD's as they cannot & will NOT BE TRUSTED to use on my work machine. I have been a BMG Music Customer for years & years. I can't trust any of them now. I cannot afford to infect my customers machines! Sony/BMG…You screwed up in my opinion and you have lost me as a customer…And ALL MY CUSTOMERS.

32. *cglrcng* Says:
November 19th, 2005 at 12:53 am

From unfinished ine in the post above….Sry.

I immediately reported that to the Sysinternals site that I received the Sony/BMG rootkit installed info from.

33. *The Sony Boycott Blog » Blog Archive » Sunncomm uninstaller vulnerabilities* Says:
November 19th, 2005 at 2:59 am

[…] In the "you have to be kidding" department: Freedom to Tinker reports that the uninstaller for Sony's other DRM scheme, MediaMax from Sony, also compromises the security of the user's system. The authors also post a detector to see if the control is on your system and a tool that both cures the infection and inoculates against the possibility of future installation. […]

34. *Stephen* Says:
November 19th, 2005 at 2:12 pm

http://netweb.wordpress.com/2005/11/20/the-sony-site-revamp

A summary of the updated web site and 'Volunary Exchange Program' with bonus MP3 versions of the aitles affected

35. *Anonymous* Says:
November 19th, 2005 at 8:33 pm

If Sony would use this type of DRM on its CDs, why wouldn't it use it on Sony VAIO computers? How can I check to see if my computer was shipped with a rootkit preinstalled?

36. *Anonymous* Says:
November 19th, 2005 at 9:50 pm

http://www.sysinternals.com/Utilities/RootkitRevealer.html

http://research.microsoft.com/rootkit/

37. *Mike* Says:
November 20th, 2005 at 10:42 pm

Sony BMG’s rootkit bungling has brought suspicion to the entire entertainment industry. Email Battles asks, “If Sony BMG can be this stupid, why not the rest? And what makes you think they stopped with rootkits?”

http://www.emailbattles.com/archive/battles/security_aacbcdjiah_ha/

38. *Bill Whitmore* Says:
November 21st, 2005 at 8:09 am

They claim to have patched the security exposure and also claim they do not collect usage data.

http://www.digitalmusicnews.com/#112105sunncomm

39. *Beta* Says:
November 22nd, 2005 at 1:37 pm

Yes, cglrcng I am very mad at Sony, I have already contacted a class action law firm — I’m in California.

On my PC, I played a music CD I had just bought at Wal Mart. A a few days later my PC starts crashing, freezing or displaying hundreds of error mesagess — as time went by, it got worse and worse.

Then I came home and found my DSL PC uploading all my personal info through my locked Zone Alarm firewall–I unplugged it.

I used another PC to go online and I found out about Sony’s rootkit and what it did to me — I am mad, very mad.

If you would like to join me in a class action suit my email is: 2star13 (at) spcglobal. net

–Beta

40. *Diogenes_Isher* Says:
November 22nd, 2005 at 11:23 pm

Hmmm, why is it my PC _never_ (really, not even once) was hit by evil programs, rootkits, virus, spyware(s/z), worms ?
Could it be because I run a *BSD/Linux system - that cannot be penetrated by sh*t_ware(s/z) made for “the most popular”
ehhh, “system” in the world ?? (There’s no way securing a “more sheeple” [burp] “system” anyway…).
Actually I wrote most of the security_programs protecting the machine myself, so anybody who wants to try crack it: be my guest (and get cracked yourself like the rest… 😉).
At least I’ll portscan you - most xp (= eXterminated Privacy) (l)users will probably not even notice that, because they don’t even know what an IDS || a stateful-packetfilter is…

My little advise to all you guys && girls: get rid of the m$ sh*t && install a _real_ system like *BSD || Linux, /etc…
(You can download these systems for _free_ see: http://www.freebsd.org/where.html for *BSD && http://www.linuxiso.org/ for Linux).
So YOU’ll be controlling your PC - not some evil corporated criminals… (That’s what they are, it’ll take some time untill everybody realizes !).
Btw. I quitted buying cds && dvds years ago, they are _way_ to expensive…

(There are some little (Hackers-)jokes hidden in this reply, see if you can find them… 😉)

Diogenes.
(Yep, the guy livin’ in an empty winebarrel 😉).

41. *got cheated by sony* Says:

November 28th, 2005 at 5:59 pm

I got the Sunncomm software after I put my CD in and said NO to the EULA - I complained to both Sony and Sunncomm and finally got them to send me a link to the uninstaller (which is the same link u can find here http://www.sunncomm.com/support/sonybmg/) - they said on the reply email that this is a “BRAND NEW UNINSTALL UTILITY” found here-

http://www.sunncomm.com/support/tools/removal.asp

but I am not sure how new it is and if it is safe to use. Does anyone know if they have closed the security hole of this uninstaller and replaced the flawed uninstaller with a safe one???

I will write back to Sunncomm to ask but no sure how they defined “safe”. Any info would help please!!!

42. *simplyshaman* Says:
December 12th, 2005 at 3:06 pm

and now we know just why it is that musicians are beginning to make the switch fom being handled by record companies… to working direct with retailers.. as garth brooks did with his new box set…

if record companies such as sonybmg are allowed to install malicious software that clearly is a breach of the privacy act… they deserve every penny of profit loss that they are about to experience as this idea takes hold…

and given the internet was invented by the united states.. there need to be enforcable controls in place to prevent this sort of thing..

i wholeheartedly agree that companies that engage in placing spyware on user’s computers without their consent should be shut down and their assets used to enforce this staple of society which we have all grown accustomed to using in our day to day lives..

make it safe.. so that it can continue to be a source of learning, and business connectivity, advertising and marketing for everyone to enjoy.

just my thoughts,
shaman

43. *Sony BMG ruft Mac-DRM nicht zur?>* Says:
January 6th, 2006 at 2:38 pm

[…] In dem Sony-R? ist allerdings nur von XCP die Rede: CDs mit dem Kopierschutz MediaMax von Sunncomm werden demnach weiter verkauft. MediaMax installiert nach Ermittlungen des Blogs Freedom to Tinker ebenfalls Dateien auf dem Mac, und zwar unabh□ig davon, ob man die Lizenzbedingungen akzeptiert oder nicht. Damit nicht genug: auch MediaMax spioniert das Verhalten des Users aus und ?ttelt - entgegen den Behauptungen der Firmen - CD- und Betriebssystemdaten an Sunncomm. […]

44. *Cat Fight! SPF Claws Sender-ID* Says:
January 7th, 2006 at 12:22 pm

[…] ::Holes! Sony CD DRM uninstaller #2: SunnComm!Freedom to Tinker […]

45. *crankademic » Blog Archive » The Canadians shall Inherit the Earth* Says:
January 7th, 2006 at 8:58 pm

[…] All this in the shadow of Sony and their Orwellian hoo-ha. Turns out the rootkit was just the tip of the iceberg. A word of advice to the moral hunchbacks who head companies firmly rooted in Cold War, hierarchal, men-in-suits-know-best business models : […]

46. *Security Fix - Brian Krebs on Computer and Internet Security - (washingtonpost.com)* Says:
January 8th, 2006 at 1:57 am

    […] And maybe it shouldn't: Security researchers — the same ones who earlier this week found serious security holes in a patch Sony issued to remove the scariest components of its anti-piracy program — today bring us evidence of similarly frightening security holes associated with another digital rights management (DRM) program the recording label uses on some CDs, a product called SunnComm MediaMax. […]

47. *Australian Open Access User Group - PC tips & tricks* Says:
January 8th, 2006 at 2:03 am

    […] 19 Nov 05 Freedom-to-tinker: Not Again! Uninstaller for Other Sony DRM Also Opens Huge Security Hole. […]

48. *PC Pro: News: Fresh security flaw found in Sony DRM component* Says:
January 9th, 2006 at 4:38 pm

    […] Halderman is working with SunnComm to test a new version of the uninstaller. More information and instructions for removing the ActiveX file can be found at in his article at www.freedom-to-tinker.com/?p=931. […]

49. *BrainLog - November 2005 Archives* Says:
January 10th, 2006 at 3:01 am

    […] AARGH! Uninstaller for Other Sony DRM Also Opens Huge Security Hole. The SunnComm software and its uninstaller is also very dangerous. […]

Leave a Reply

Name

Mail (will not be published)

Website

Submit Comment

Powered by WordPress.
Entries (RSS) | Comments (RSS).